Versión 7 de diciembre de 2017

FORO HEMISFÉRICO DE COOPERACIÓN INTERNACIONAL CONTRA EL DELITO CIBERNÉTICO

Santo Domingo, República Dominicana, 5 al 7 de diciembre de 2017

organizado por

el Gobierno de la República Dominicana, el Consejo de Europa y la Unión Europea por medio del proyecto conjunto GLACY+, la Organización de los Estados Americanos a través del Departamento de Cooperación Jurídica (Secretaría Técnica de las REMJA) y el Departamento de Justicia de Estados Unidos con el apoyo de la Unión Europea, INTERPOL, AMERIPOL, el Departamento de Justicia de Canadá, CARICOM y el Foro Mundial de Competencia Cibernética

Resumen del foro

Más de 150 representantes de gobiernos y autoridades de la justicia penal de [34] países y territorios de las Américas, el sector privado y organizaciones internacionales participaron en el Foro Hemisférico de Cooperación Internacional contra el Delito Cibernético, que tuvo lugar en Santo Domingo, República Dominicana, del 5 al 7 de diciembre de 2017.

Participaron los siguientes países y territorios: Antigua y Barbuda, Argentina, Bahamas, Barbados, Belize, Bermudas, Bolivia, Brasil, Canadá, Islas Caimán, Chile, Colombia, Costa Rica, Curazao, Ecuador, El Salvador, Estados Unidos, Grenada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Montserrat, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Santa Lucía, San Martín, Suriname y Uruguay.

Participaron las siguientes organizaciones e iniciativas internacionales: AMERIPOL, CARICOM, CARICOM IMPACS, Consejo de Europa, Unión Europea, Foro Mundial de Competencia Cibernética, INTERPOL, Sistema de Seguridad Regional y Organización de los Estados Americanos.

Presentaron su experiencia oradores de Argentina, Canadá, Consejo de Europa, el Departamento de Justicia de Estados Unidos, Foro Global de Ciberexpertos, Guatemala, INTERPOL, Sistema de Seguridad Regional, República Dominicana y Microsoft.

La finalidad del Foro era que los países participantes pudieran aprovechar mejor los programas de aumento de la capacidad que ofrecen las organizaciones internacionales, a fin de aumentar la cooperación y la sinergia entre organizaciones e iniciativas internacionales y dar a conocer experiencias con el fortalecimiento de las actividades de aumento de la capacidad de las autoridades en el ámbito de la justicia penal.

Cabe destacar los siguientes mensajes fundamentales del Foro:

- El delito cibernético y los asuntos relacionados con las pruebas electrónicas socavan las oportunidades que ofrece la tecnología de la información para el desarrollo social y económico, así como los derechos humanos, la democracia y el estado de derecho. Se necesita una respuesta y una cooperación más eficaces de la justicia penal en todos los niveles.

- Lo mismo puede decirse de la cooperación entre organizaciones internacionales. Una mayor cooperación les permitiría prestar el mejor servicio posible a los Estados. El Foro en sí fue una muestra de lo que se puede lograr cuando las organizaciones internacionales aúnan fuerzas para apoyar a países y territorios del hemisferio en su labor para superar el reto del delito cibernético.

- La legislación sobre el delito cibernético y las pruebas electrónicas constituye la base de una respuesta de ese tipo. Un número creciente de países de las Américas han adoptado o están adoptando leyes internas, guiándose a menudo por el Convenio de Budapest sobre la Ciberdelincuencia. Cabe destacar que el Consejo de Europa, con el proyecto GLACY+, está en condiciones de apoyar en este proceso a los países de la región que lo soliciten.

- El aumento de la capacidad es una manera eficaz de que los países fortalezcan la legislación, la capacidad institucional y la cooperación en todos los niveles. Cabe señalar los siguientes ejemplos de buenas prácticas y ofrecimientos de apoyo:

    - El proyecto de Acción Mundial sobre el Delito Cibernético Extendido (GLACY+) de la Unión Europea y el Consejo de Europa;
    - El Programa de Cooperacion Juridica de la Organización de Estados Americanos dentro del marco de los mandatos de la REMJA (Reuniones de Ministros de Justicia y Procuradores de las Americas).
    - UNODC Programa Global en Cibercrimen.
    - Proyecto "Cyber Américas" de INTERPOL finaciado por el Gobierno de Canadá.
    - Cursos de certificación como la fuente de datos del ICSE (Explotación sexual infantil internacional) y la plataforma del ICCACOPS por el INTERPOL y USDOJ. Los Estados exaltaron la utilidad de la certificación de policías practicantes.

- Cooperación con el sector privado

    - Reconociendo que la ciberseguridad y el combate del delito cibernético son temas que interesan a todos, sería conveniente contar con una plataforma que facilite un alto grado de cooperación entre los sectores público y privado. Actualmente, los cambios geopolíticos, la aceleración de los adelantos tecnológicos y la evolución de los ataques han creado una brecha entre las políticas en materia de respuesta y su ejecución efectiva en tiempo real. Es necesario que todas las partes participen en la creación de un marco jurídico pragmático que posibilite la aplicación de las leyes, protegiendo al mismo tiempo la privacidad individual y facilitando la cooperación entre países.

    - INTERPOL está enfocando sus recursos para expandir sus acuerdos de intercambio de información con el sector privado para producir inteligencia para los Estados miembros. Países participantes en el "Cyber Surge" solicitaron al INTERPOL para que continúe produciendo y diseminando inteligencia a través de los canales apropiados.

- La web oscura, bitcoin y los flujos ilícitos de dinero

    - Los casos vinculados a la ciberdelincuencia son complicados y requieren tenacidad, recursos, inteligencia y paciencia de los investigadores, así como la coordinación entre las distintas entidades gubernamentales, para el éxito del rastreo, la investigación, la captura y el enjuiciamiento de criminales.
    - En ocasiones, los delincuentes cometen errores que pueden deben ser utilizados para capturarlos y enjuiciarlos.
    - La cooperación internacional en casos relacionados con los delitos cibernéticos es muy importante, especialmente para el intercambio de experiencias y asistencia técnica en casos que países no habían observado anteriormente.
    - Los investigadores y fiscales tienen la responsabilidad de explicar los aspectos técnicos de temas complejos en términos claros y sencillos a los jueces y a los jurados.

- Acceso a pruebas en la nube

    - En vista de que, en medida creciente, se almacenan pruebas electrónicas en servidores en la nube, se necesitan medidas específicas para protegerlas para su uso en el ámbito de la justicia penal. En ese sentido cabe destacar el trabajo del Comité del Convenio contra la Ciberdelincuencia en el marco del Convenio de Budapest, incluida la negociación de un protocolo sobre el acceso a pruebas en la nube, que comenzó en septiembre de 2017. Asimismo, cabe señalar que las entidades del sector privado están dispuestas a cooperar con las autoridades públicas. Los gobiernos podrían considerar la posibilidad de dar seguimiento al trabajo del Comité del Convenio contra la Ciberdelincuencia relativo a un protocolo al Convenio de Budapest y de adherirse a este tratado.

- Cooperación entre organizaciones internacionales

    - Los avances en la conciencia nacional e internacional constituyen las bases de una acción eficaz. Es necesario revaluar y renovar en la medida de lo posible los marcos jurídicos internacionales, ofrecer un foro para un diálogo internacional más amplio con miras a aumentar y promover la cooperación policial y judicial internacional, entre las autoridades nacionales y entre organizaciones internacionales y regionales. En esta tarea se debería tener en cuenta la influencia de temas nuevos y emergentes en el ámbito de la cooperación policial y judicial internacional en asuntos penales y formular recomendaciones sobre el aumento de la capacidad, mostrando igual preocupación por la situación en los países que se encuentran en distintas etapas de desarrollo, a fin de evitar un futuro caótico.

En cuanto al camino por delante:

- Los Estados deberían adoptar marcos jurídicos internos apropiados para el delito cibernético y las pruebas electrónicas, en concordancia con normas internacionales tales como el Convenio de Budapest.

- Los Estados, con el apoyo de organizaciones internacionales, deben seguir aumentando la capacidad y las aptitudes de los órganos policiales, las fiscalías y el poder judicial.

- Las autoridades de la justicia penal deben fortalecer la cooperación con el sector privado a fin de posibilitar el acceso oportuno a los datos.

- Hay que agilizar los procedimientos para la tramitación de pedidos de asistencia jurídica recíproca. Los Estados podrían considerar la posibilidad de adherirse al Convenio de Budapest como marco para la cooperación internacional.

- Las organizaciones internacionales deben intensificar la cooperación entre ellas y buscar sinergia en las actividades de aumento de la capacidad.

- Los oradores recalcaron una y otra vez la importancia de la comunicación y la cooperación entre los gobiernos y el sector privado, particularmente en el caso de los países que todavía no han establecido relaciones firmes con proveedores comunes.

- Hubo acuerdo entre los participantes sobre la necesidad de trabajar en estrategias de aumento de la capacidad de los operadores del sistema de justicia penal en lo que concierne a los retos que plantean los delitos informáticos y las pruebas digitales. También es necesario promover cursos interdisciplinarios con un contenido jurídico y técnico, así como la formación de instructores en los distintos países de la región y un mejor aprovechamiento de los recursos para la cooperación internacional.

- Se reconoció la importancia de crear fiscalías especializadas en delitos cibernéticos y promover actividades conjuntas y nexos entre fiscalías especializadas en el ámbito regional.

- Se reconoció la necesidad de una nueva rama del derecho procesal penal que se ocupe de las pruebas digitales y la creación de facultades procesales. Se recomendó usar como guía el Convenio de Budapest.

- Se aceptó la necesidad urgente de trabajar en una nueva normativa (a escala internacional y nacional) con respecto al acceso transfronterizo a los datos, así como al acceso a los datos en la nube. Asimismo, se consideró crucial la conclusión de un protocolo al Convenio de Budapest sobre la preservación de datos, las órdenes de presentación de datos, y el registro y la incautación cuando los datos se encuentran en otra jurisdicción.

- Se consideró importante promover normas con respecto a la cooperación voluntaria transfronteriza de proveedores de servicios de Internet (cooperación asimétrica).

Los participantes agradecieron la forma en se organizó la conferencia y la calidad de las intervenciones de los oradores.